

CLAIMS

What is claimed is:

5 1. A method of creating a certificate revocation list (CRL), comprising:

 a) creating a single CRL that is centralized, said single CRL associated with a certificate authority (CA) comprising a master server coupled to a plurality of CA clone
10 servers;

 b) maintaining said single CRL with said master server;

 c) receiving notice, from one of said plurality of CA clone servers, at said master server containing revocation information regarding a certificate; and

15 d) updating said single CRL according to said revocation information.

 2. The method of creating a CRL as described in Claim 1, wherein step d) comprises:

20 adding said certificate to said single CRL when said revocation information indicates said certificate is revoked, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.

25 3. The method of creating a CRL as described in Claim 1, wherein step d) comprises:

removing said certificate from said single CRL when said revocation information indicates said certificate is valid, said revocation information associated with a revocation event occurring at one of said plurality of CA clone servers.

5

4. The method of creating a CRL as described in Claim 1, further comprising:

maintaining said single CRL with a CRL merger service module located at said master server.

10

5. The method of creating a CRL as described in Claim 1, further comprising:

sending said notice over a secure communications channel.

15

6. The method of creating a CRL as described in Claim 5, further comprising:

at said one of said cluster of servers, performing secure sockets layer (SSL) client authentication over said secure communications channel before sending said notice over said secure communications channel.

20

7. The method of creating a CRL as described in Claim 1, further comprising:

25

transmitting said single CRL that is updated to a recipient over a communication network.

8. The method of creating a CRL as described in Claim
1, further comprising:

providing certificate authority services not including
maintaining and managing said single CRL at each of said
5 plurality of CA clone servers.

9. The method of creating a CRL as described in Claim
1, further comprising:

storing said CRL in a database accessed via a
10 lightweight directory access protocol (LDAP) that supports a
Secure Sockets Layer (SSL).

10. The method of creating a CRL as described in Claim
1, further comprising:

15 at said one of said plurality of clone servers,
detecting whether said notice was received at said master
server;

repeatedly sending said notice until received by said
master server.

20

11. The method of creating a CRL as described in claim
10, further comprising:

storing said notice if said notice was not received at
said master server.

25

12. In a certificate authority (CA) having a plurality of clone servers, a method generating and maintaining certificate revocation list information, comprising:

a) each of said clone servers independently generating
5 revocation information relating to certificates;

b) sending said revocation information to a master server coupled to said plurality of clone servers; and

c) maintaining a single centralized certificate revocation list (CRL) based on said revocation information
10 from said plurality of clone servers, said step c) performed by said master server.

13. The method as described in Claim 12, further comprising:

d) in response to an inquiry for said CRL, providing
15 said CRL on behalf of said CA, said step d) performed by said master server.

14. The method as described in Claim 12, further
20 comprising:

d) based on said revocation information, adding a certificate to said CRL when said revocation information indicates said certificate is revoked.

25 15. The method as described in Claim 12, further comprising:

d) based on said revocation information, removing a certificate from said CRL when said revocation information indicates said certificate is valid.

5 16. A certificate authority (CA) comprising:

 a plurality of clone servers coupled together for providing certificate authority services;

 a centralized certificate revocation list (CRL) associated with said CA; and

10 a master server coupled to said plurality of clone servers for maintaining said centralized CRL based on revocation information from said plurality of clone servers.

15 17. The CA as described in Claim 16, wherein said master server adds a certificate to said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate has been revoked.

20 18. The CA as described in Claim 16, wherein said master server removes a certificate from said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate is valid.

25 19. The CA as described in Claim 16, further comprising:

a secure communication network coupling each of said plurality of clone servers to said master server for providing secure communication when said information is sent between said plurality of clone servers and said master
5 server.

20. The CA as described in Claim 16, further comprising:

a lightweight directory access protocol (LDAP) database
10 that is coupled to said master server for storing said centralized CRL.

21. The CA as described in Claim 16, further comprising:

15 a CRL merger service module located at said master server for maintaining said CRL.

22. A certificate authority (CA) comprising:

a plurality of clone servers coupled together for
20 providing certificate authority services;

a centralized certificate revocation list (CRL) associated with said CA, said centralized CRL located in a lightweight directory access protocol (LDAP) database; and

a master server coupled to said plurality of clone
25 servers for maintaining said centralized CRL based on revocation information from said plurality of clone servers, said centralized CRL coupled to said merger server.

23. The CA as described in Claim 22, wherein said master server adds a certificate to said centralized CRL after said revocation information by one of said plurality of clone servers indicates that said certificate has been
5 revoked.

24. The CA as described in Claim 22, wherein said master server removes a certificate from said centralized CRL
10 after said revocation information by one of said plurality of clone servers indicates that said certificate is valid.